DEFENSE INFORMATION SYSTEMS AGENCY
JOINT INTEROPERABILITY TEST COMMAND
P.O. BOX 12798
FORT HUACHUCA, ARIZONA 85670-2798

IN REPLY
REFER TO: Battlespace Communications Portfolio (JTE)

MEMORANDUM FOR DISTRIBUTION 10 December 2007

SUBJECT: Special Interoperability Test Certification of the Foundry Assured Services Voice Application Local Area Network (ASVALAN) and Voice Application Local Area Network (VALAN) with Specified Software Releases

References: (a) DoD Directive 4630.5, "Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)," 5 May 2004
(b) CJCSI 6212.01D, "Interoperability and Supportability of Information Technology and National Security Systems," 8 March 2006

1. References (a) and (b) establish the Defense Information Systems Agency (DISA), Joint Interoperability Test Command (JITC), as the responsible organization for interoperability test certification. Additional references are provided in enclosure 1.

2. The Foundry ASVALAN and VALAN with Specified Software Releases is hereinafter referred to as the system under test (SUT). The SUT meets all of its critical interoperability requirements and is certified as interoperable for joint use within the Defense Switched Network (DSN). The SUT is certified for joint use within the DSN with the Digital Switching Systems on the DSN Approved Products List (APL) which are certified for use with an ASVALAN or VALAN. The SUT components which are bolded and underlined in the tables throughout this certification letter are components that were tested in the JITC laboratory for this certification. The SUT components which are not bolded and not underlined, but also listed throughout the tables in this letter, are certified for joint use in the DSN as well. The JITC analysis determined these components contain the same hardware and software and are functionally identical to the tested components for interoperability certification purposes. The SUT is certified to support DSN assured services over Internet Protocol as an ASVALAN. If a system meets the minimum requirements for an ASVALAN, it also meets the lesser requirements for a VALAN. However, since VALANs do not support the Assured Services Requirements detailed in reference (c), Command and Control (C2) users and Special C2 users are not authorized to be served by a VALAN. Since VALANs do not support Assured Services, they can only serve Department of Defense (DoD), non-DoD, non-governmental, and foreign government users having no missions or communications requirement to ever originate or receive C2 communications. VALAN connectivity to the DSN is not authorized until a waiver is granted by the Joint Staff for each site. The SUT is certified for joint use as a VALAN for non-C2 traffic. The VALAN requirements differing from those of an ASVAL include:

- C2 traffic shall not traverse a VALAN.
- Reliability is a conditional requirement for a VALAN.

- Network Management features are conditional requirements for a VALAN.

Testing did not include video services or data applications; however, simulated data traffic was generated during testing to determine its effect on voice traffic. This certification expires upon changes that could affect interoperability, but no later than three years from the date of this memorandum.

3. This finding is based on interoperability testing conducted by JITC and a review of the vendor's Letters of Compliance (LoC). Testing was conducted at JITC's Global Information Grid Network Test Facility at Fort Huachuca, Arizona, from 23 July through 31 August 2007. Review of the vendor's LoC was completed on 5 October 2007. Enclosure 2 documents the test results and describes the tested network. System interoperability should be verified before deployment in an operational environment that varies significantly from the test environment.

4. The overall interoperability status of the SUT is indicated in table 1. The ASVALAN and VALAN system requirements are listed in table 2. In addition to system level requirements, components that comprise the SUT must meet specific criteria to be certified for use as core, distribution, or access components. The interoperability status of the SUT components is listed in table 3. The ASVALAN and VALAN requirements used to certify the components are listed in table 4. This interoperability test status is based on the SUT's ability to meet:

a. Assured services as defined in reference (c).

b. Local Area Network system requirements specified in reference (d) verified through JITC testing and/or vendor submission of LoC.

c. Internet Protocol version 6 requirements specified in reference (d), paragraph 1.7, table 1-4, verified through vendor submission of LoC signed by the Vice President of the company.

d. The overall system interoperability performance derived from test procedures listed in reference (e).

Table 1. SUT Interoperability Status

System Interoperability Status			
Components (See note.)	**Release**	**Status**	**Remarks**
Foundry NetIron XMR 4000/**8000**/16000/32000	3.3.0e	Certified	All ASVALAN and VALAN system requirements were met when the SUT was configured in accordance with architecture provided in enclosure 2. Additional details about component level certification are provided in table 3. Security testing is accomplished through DISA-led Information Assurance Test teams and published in a separate report.
Foundry NetIron MLX 4/**8**/16/32	3.3.0e		
Foundry BigIron RX 4/**8**/16/32	2.3.0e		
Foundry BigIron 4000/8000/15000	8.0.01k		
FastIron SX 800/SX 1600	3.3.00		
FastIron FESX424-PoE/ FESX424/FESX424HF/ FESX448	3.3.00		
FastIron GS648P-PoE GS624P-PoE/LS648/LS624	3.2.00		
FastIron Edge 4802-PoE/2402-PoE	3.7.00a		

LEGEND:
ASVALAN - Assured Services Voice Application Local Area Network
DISA - Defense Information Systems Agency
JITC - Joint Interoperability Test Command
PoE - Power over Ethernet
SUT - System Under Test
VALAN - Voice Application Local Area Network

NOTE: Components bolded and underlined were tested by JITC. The other components in the family series were not tested; however, they utilize the same software and hardware and JITC analysis determined them to be functionally identical for interoperability certification purposes and they are also certified for joint use.

Table 2. ASVALAN and VALAN System Requirements

System Requirements				
Requirement	**Criteria**		**Reference**	**Required**
Delay	One-way packet delay for voice packets of an established call (signaling and media) shall be 5 ms or less averaged over any 5-minute period.		GSCR, Appendix 3, Section A.3.3.1.1	Yes
Jitter	For voice media packets, jitter shall be 5 ms or less averaged over any 5-minute period.		GSCR, Appendix 3, Section A.3.3.1.2	Yes
Packet Loss	Voice packet loss within the LAN shall not exceed 0.05% averaged over any 5-minute period.		GSCR, Appendix 3, Section A.3.3.1.3	Yes
Reliability	ASVALAN	- ASVALANs shall have a reliability of .99999 - No single point of failure for outage of more than 64 telephony subscribers - Network Path restores within 2 seconds	GSCR, Appendix 3, Section A.3.3.4.1	Yes
	VALAN	- This requirement is conditional for a VALAN.	GSCR, Appendix 3, Section A.3.3.4.1	No
IPv6[1]	All IP devices shall be IPv6 capable.		GSCR, Paragraph 1.7, and GSCR Appendix 3, Section A3.2.8	Yes
Security[2]	DIACAP (replacement for DITSCAP)/IA		GSCR, Appendix 3, Section A.3.3.4.3	Yes

LEGEND:
ASVALAN - Assured Services Voice Application LAN
DIACAP - DoD IA Certification and Accreditation Process
DISA - Defense Information Systems Agency
DITSCAP - DoD IT Security Certification and Accreditation Process
DoD - Department of Defense
GSCR - Generic Switching Center Requirements
IA - Information Assurance
IP - Internet Protocol
IPv4 - Internet Protocol version 4
IPv6 - Internet Protocol version 6
IT - Information Technology
LAN - Local Area Network
ms - milliseconds
VALAN - Voice Application LAN

NOTES:
1 An IPv6 capable system or product, as defined in the GSCR, paragraph 1.7, shall be capable of receiving, processing, and forwarding IPv6 packets and/or interfacing with other systems and protocols in a manner similar to that of IPv4. IPv6 capability is currently satisfied by a vendor Letter of Compliance signed by the Vice President of the company. The vendor must state, in writing, compliance to the following criteria by**:**
a. Conformant with IPv6 standards profile contained in the DoD IT Standards Registry (DISR).
b. Maintaining interoperability in heterogeneous environments and with IPv4.
c. Commitment to upgrade as the IPv6 standard evolves.
d. Availability of contractor/vendor IPv6 technical support.
2 Security testing is accomplished via DISA-led Information Assurance test teams and published in a separate report.

Table 3. SUT Component Interoperability Status

Component Interoperability Status					
Component (See note.)	**Release**	**Sub-component** (See note.)	**Status**	**Layer (s)**	**Remarks**
Foundry NetIron XMR 4000/**8000**/16000/32000	3.3.0e	**NI-XMR-MR**	Certified	Core, Distribution, Access	All CRs and FRs were met.
		NI-XMR-32-MR	Certified		
		NI-X-SF1	Certified		
		NI-X-SF3	Certified		
		NI-X-32-SF	Certified		
		NI-XMR-10Gx4	Certified		
		NI-XMR-10Gx2	Certified		
		NI-XMR-1Gx20-SFP	Certified		
		NI-XMR-1Gx20-GC	Certified		
Foundry NetIron MLX 4/**8**/16/32	3.3.0e	**NI-XMR-MR**	Certified	Core, Distribution Access	All CRs and FRs were met.
		NI-XMR-32-MR	Certified		
		NI-X-SF1	Certified		
		NI-X-SF3	Certified		
		NI-X-32-SF	Certified		
		NI-XMR-10Gx4	Certified		
		NI-XMR-10Gx2	Certified		
		NI-XMR-1Gx20-SFP	Certified		
		NI-XMR-1Gx20-GC	Certified		
Foundry BigIron RX 4/**8**/16/32	2.3.0e	**RX-BI-MR**	Certified	Distribution Access	All CRs and FRs were met.
		RX-BI-MR2	Certified		
		RX-BI-32-MR	Certified		
		RX-BI-32-MR2	Certified		
		RX-BI-SFM1	Certified		
		RX-BI-SFM3	Certified		
		RX-BI-32-SFM	Certified		
		RX-BI2XG	Certified		
		RX-BI4XG	Certified		
		RX-BI24C	Certified		
		RX-BI24HF	Certified		
		RX-BI48T	Certified		
Foundry BigIron 4000/8000/15000	8.0.01k	**J-BxGMR4**	Certified	Distribution Access	All CRs and FRs were met.
		J-B2GMR4	Certified		
		J-BxG	Certified		
		J-B16Gx	Certified		
		J-B16GC	Certified		
		J-B48E	Certified		
		J-B48T	Certified		
FastIron SX 800/SX 1600	3.3.00	**SX-FIZMR**	Certified	Access	All CRs and FRs were met.
		SX-FI424F	Certified		
		SX-FI42XG	Certified		
		SX-FI42XGW	Certified		
		SX-FI424P	Certified		
		SX-FI424C	Certified		
		FI-FISF	Certified		
FastIron FESX424-PoE/FESX424/FESX424HF/FESX448	3.3.00	Not Applicable	Certified	Access	All CRs and FRs were met.

Table 3. SUT Component Interoperability Status (continued)

Component Interoperability Status					
Component (See note.)	**Release**	**Sub-component** (See note.)	**Status**	**Layer (s)**	**Remarks**
FastIron GS648P-PoE/GS624P-PoE/LS648/LS624	3.2.00	Not Applicable	Certified	Access	All CRs and FRs were met.
FastIron Edge 4802-PoE/2402-PoE	3.7.00a	Not Applicable	Certified	Access	All CRs and FRs were met.

LEGEND:
CRs - Capability Requirements
FRs - Feature Requirements
JITC - Joint Interoperability Test Command
PoE - Power over Ethernet
SUT - System Under Test

NOTE: Components bolded and underlined were tested by JITC. The other components in the family series were not tested; however, they utilize the same software and hardware and JITC analysis determined them to be functionally identical for interoperability certification purposes and they are also certified for joint use.

Table 4. ASVALAN and VALAN Component Requirements

Core/Distribution/Access Component Requirements				
Requirement	**Criteria**		**Reference**	**Required**
CoS Models	LAN components shall support IEEE 802.1p to DSCP mapping and at least one of the following: - IEEE 802.1p/Q priority tagging/VLAN tagging - DSCP - ToS		GSCR, Appendix 3, Section A.3.3.2.1	Yes
Traffic Prioritization	Traffic within LAN components shall be prioritized so that voice signaling receives highest priority, voice media second highest priority, and data lowest priority.		GSCR, Appendix 3, Section A.3.3.2.2	Yes
QoS	LAN components shall support one of the following: - Priority Queuing - Custom Queuing - Weighted Fair Queuing - Class Based Weighted Fair Queuing		GSCR, Appendix 3, Section A.3.3.3.1	Yes
Policing	LAN components shall support one of the following: - DSCP PHB - Generic Traffic Shaping - Class-Based Shaping		GSCR, Appendix 3, Section A.3.3.3.2	Yes
VLANs	LAN components shall support: - Port based VLANs - MAC address based VLANs - Protocol based VLANs		GSCR, Appendix 3, Section A.3.3.3.3	Yes
IEEE Conformance	LAN components shall support: - IEEE 802.1d – Bridging - IEEE 802.1p/Q – Priority tagging/VLAN tagging - IEEE 802.1s – Per-VLAN Group Spanning Tree - IEEE 802.1v – VLAN Classification by port and protocol - IEEE 802.1w –Rapid Reconfiguration of Spanning Tree - IEEE 802.1x – Port Based Network Access Control - IEEE 802.3ad – Link Aggregation Protocol		GSCR, Appendix 3, paragraph A.3.3.4	Yes
Reliability	ASVALAN	LAN components shall support: - ASVALAN components shall have a reliability of .99999 or better - Dual power supplies and dual processors (more than 64 users) - N+1 sparing for access (more than 64 users) - Redundancy protocol[1] - 2 second path restoral	GSCR, Appendix 3, Section A.3.3.4.1	Yes
	VALAN	This requirement is conditional for a VALAN.	GSCR, Appendix 3, Section A.3.3.4.1	No

Table 4. ASVALAN and VALAN Component Requirements (Continued)

Core/Distribution/Access Component Requirements				
Requirement	**Criteria**		**Reference**	**Required**
Network Management	ASVALAN	LAN components shall support: - In-band or out-of-band management - SNMP - Measurements	GSCR, Appendix 3, Section A.3.3.4.2	Yes
	VALAN	This requirement is conditional for a VALAN.	GSCR, Appendix 3, Section A.3.3.4.2	No
Security	LAN components shall employ the Network Infrastructure and VoIP STIGs.[2]		GSCR, Appendix 3, Section A.3.3.4.3	Yes
IPv6	All IP devices shall be IPv6 capable.[3]		GSCR, Paragraph 1.7, and GSCR Appendix 3, Section A3.2.8	Yes
TE	ASVALAN	- ASVALAN components shall be engineered for a maximum of 25% voice traffic per link.[4] - For more than 64 users, link pairs (redundant links) must be used.	GSCR, Appendix 3, Section A.3.3.4.4	Yes
	VALAN	VALAN components shall be engineered for a maximum of 25% voice traffic per link.[4]	GSCR, Appendix 3, Section A.3.3.4.4	Yes

LEGEND:

802.1d	- Standard for Local and Metropolitan Area Networks: MAC Bridges
802.1p	- LAN Layer 2 QoS/CoS Protocol for Traffic Prioritization
802.1Q	- Standards for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks
802.1s	- Standard for Local and Metropolitan Area Networks - Amendment 3 to 802.1Q Virtual Bridged Local Area Networks: Multiple Spanning Trees
802.1v	- Standard for Local and Metropolitan Area Networks - Virtual Bridge Local Area Networks - Amendment 2: VLAN Classification by Protocol and Port (Amendment to IEEE 802.1Q, 1998 Edition)
802.1w	- Standard for Local and metropolitan area networks - Common Specifications - Part 3: Media Access Control (MAC) Bridges: Rapid Configuration
802.1x	- Standard for Local and Metropolitan Area Networks Port-Based Network Access Control
802.3ad	- Standard for Information Technology – Local and Metropolitan Area Networks – Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications–Aggregation of Multiple Link Segments
ASVALAN	- Assured Services Voice Application LAN
CoS	- Class of Service
DISA	- Defense Information Systems Agency
DSCP	- Differentiated Services Code Point
GSCR	- Generic Switching Center Requirements
IEEE	- Institute of Electrical and Electronics Engineers, Inc.
IP	- Internet Protocol
IPv4	- Internet Protocol version 4
IPv6	- Internet Protocol version 6
LAN	- Local Area Network
MAC	- Media Access Control
Mbps	- Megabits per second
N	- total VoIP users / 64
OSPFV.3	- Open Shortest-Path First Version 3
PHB	- Per Hop Behaviors
QoS	- Quality of Service
SNMP	- Simple Network Management Protocol
STIGs	- Security Technical Implementation Guides
TE	- Traffic Engineering
ToS	- Type of Service
VALAN	- Voice Application LAN
VLANs	- Virtual LANs
VoIP	- Voice over Internet Protocol
VRRP	- Virtual Router Redundancy Protocol

NOTES:

1 For core and distribution components, OSPF V.3 redundancy protocol shall be the routing protocol supported. For access components, redundancy protocol shall be VRRP or equivalent protocol.

2 Verified using the Information Assurance Test Plan. Results of the security testing are published in a separate test report generated by the DISA Information Assurance test personnel.

3 An IPv6 capable system or product, as defined in the GSCR, paragraph 1.7, shall be capable of receiving, processing, and forwarding IPv6 packets and/or interfacing with other systems and protocols in a manner similar to that of IPv4. IPv6 capability is currently satisfied by a vendor Letter of Compliance signed by the Vice President of the company. The vendor must state, in writing, compliance to the following criteria**:**

a. Conformant with IPv6 standards profile contained in the Department of Defense Information Technology Standards Registry (DISR).
b. Maintaining interoperability in heterogeneous environments and with IPv4.
c. Commitment to upgrade as the IPv6 standard evolves.
d. Availability of contractor/vendor IPv6 technical support.

4 Instruments connected to an access device must provide a minimum of a 10 Mbps full duplex link. For core and distribution connections, the minimum link capacity is 100 Mbps full duplex.

5. No detailed test report was developed in accordance with the Program Manager's request. JITC distributes interoperability information via the JITC Electronic Report Distribution (ERD) system, which uses Unclassified-But-Sensitive Internet Protocol Router Network (NIPRNet) e-mail. More comprehensive interoperability status information is available via the JITC System Tracking Program (STP). The STP is accessible by .mil/gov users on the NIPRNet at https://stp.fhu.disa.mil. Test reports, lessons learned, and related testing documents and references are on the JITC Joint Interoperability Tool (JIT) at https://jit.fhu.disa.mil (NIPRNet), or http://199.208.204.125 (SIPRNet). Information related to DSN testing is on the Telecom Switched Services Interoperability (TSSI) website at http://jitc.fhu.disa.mil/tssi.

6. The JITC point of contact is Mr. Edward Mellon, DSN 879-5159, commercial (520) 538-5159, FAX DSN 879-4347, or e-mail to Edward.Mellon@disa.mil. The tracking number for the SUT is 0703801.

FOR THE COMMANDER:

2 Enclosures a/s

RICHARD A. MEADOR
Chief
Battlespace Communications Portfolio

Distribution:
Joint Staff J6I, Room 1E596, Pentagon, Washington, DC 20318-6000
Joint Interoperability Test Command, Liaison, ATTN: TED/JT1, 2W24-8C, P.O. Box 4502, Falls Church, VA 22204-4502
Defense Information Systems Agency, Net-Centricity Requirements and Assessment Branch, ATTN: GE333, Room 244, P.O. Box 4502, Falls Church, VA 22204-4502
Office of Chief of Naval Operations (N71CC2), CNO N6/N7, 2000 Navy Pentagon, Washington, DC 20350
Headquarters U.S. Air Force, AF/XICF, 1800 Pentagon, Washington, DC 20330-1800
Department of the Army, Office of the Secretary of the Army, CIO/G6, ATTN: SAIS-IOQ, 107 Army Pentagon, Washington, DC 20310-0107
U.S. Marine Corps (C4ISR), MARCORSYSCOM, 2200 Lester St., Quantico, VA 22134-5010
DOT&E, Net-Centric Systems and Naval Warfare, 1700 Defense Pentagon, Washington, DC 20301-1700
U.S. Coast Guard, CG-64, 2100 2nd St. SW, Washington, DC 20593
Defense Intelligence Agency, 2000 MacDill Blvd., Bldg 6000, Bolling AFB, Washington, DC 20340-3342
National Security Agency, ATTN: DT, Suite 6496, 9800 Savage Road, Fort Meade, MD 20755-6496
Director, Defense Information Systems Agency, ATTN: GS235, Room 5W24-8A, P.O. Box 4502, Falls Church, VA 22204-4502
Office of Assistant Secretary of Defense (NII)/DoD CIO, Crystal Mall 3, 7th Floor, Suite 7000, 1851 S. Bell St., Arlington, VA 22202
Office of Under Secretary of Defense, AT&L, Room 3E144, 3070 Defense Pentagon, Washington, DC 20301
U.S. Joint Forces Command, J68, Net-Centric Integration, Communications, and Capabilities Division, 1562 Mitscher Ave., Norfolk, VA 23551-2488
Defense Information Systems Agency (DISA), ATTN: GS23 (Mr. McLaughlin), Room 5W23, 5275 Leesburg Pike (RTE 7), Falls Church, VA 22041

ADDITIONAL REFERENCES

(c) Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6215.01B, "Policy for Department of Defense Voice Services," 23 September 2001

(d) Defense Information Systems Agency (DISA), "Defense Switched Network (DSN) Generic Switching Center Requirements (GSCR), Appendix 3, Errata Change 2," 14 December 2006, Revised 27 March 2007

(e) Joint Interoperability Test Command, "Defense Switched Network Generic Switch Test Plan (GSTP), Change 2," 2 October 2006

CERTIFICATION TESTING SUMMARY

1. SYSTEM TITLE. Foundry Assured Services Voice Application Local Area Network (ASVALAN) and Voice Application Local Area Network (VALAN) with Specified Software Releases; hereinafter referred to as the system under test (SUT).

2. PROPONENT. White House Communications Agency (WHCA).

3. PROGRAM MANAGER. Lt Col Alain L. M. Jones, WHCA/J5, 2743 Defense Blvd, Anacostia Annex, District of Columbia, 20373, e-mail: ALJones@whmo.mil.

4. TESTER. Joint Interoperability Test Command (JITC), Fort Huachuca, Arizona.

5. SYSTEM UNDER TEST DESCRIPTION. The SUT is used to transport voice signaling and media as part of an overall Voice over Internet Protocol (VoIP) system. All of the SUT switches provide availability, security, and Quality of Service (QoS) to meet the operational requirements of the network and Assured Services for the warfighter. The SUT components which are bolded and underlined in the tables throughout this certification letter, are components that were tested in the JITC laboratory for this certification. The SUT components which are not bolded and not underlined but also listed throughout the tables in this letter, were determined by JITC analysis to contain the same hardware and software as, and to be functionally identical to, the tested components for interoperability certification purposes. The SUT is certified for joint use within the Defense Switched Network (DSN) with the Digital Switching Systems on the DSN Approved Products List (APL), which are certified for use with an ASVALAN or VALAN. The SUT is certified to support DSN assured services over Internet Protocol (IP) as an ASVALAN.

The SUT is composed of the following components:

The NetIron XMR, NetIron MLX, and BigIron RX series deliver scalable performance and port density across several chassis configurations. The NetIron XMR, NetIron MLX, and BigIron RX series are available in a 4-, 8-, 16-, and 32-slot chassis. These switches feature a range of integrated services modules, including 10-gigabit fiber, 1-gigabit fiber, and 10/100/1000BaseT modules. For data and voice applications, users can connect to the Local Area Network (LAN) using the 10/100/1000BaseT Ethernet interface on the access devices. The NetIron XMR and MLX series switches are certified in the core, distribution, and access layers when deployed as a component in an ASVALAN or VALAN, while the BigIron RX is certified in the distribution and access layers. The NetIron XMR, NetIron MLX, and BigIron RX series were tested for 100/1000/10000 Megabits per second (Mbps) data load throughput. The NetIron XMR, NetIron MLX, and BigIron RX series met all Internet Protocol version 4(IPv4) and Internet Protocol version 6 (IPv6) and Core requirements.

The BigIron series delivers scalable performance and port density across several chassis configurations. The BigIron series is available in a 4-, 8-, and 15-slot chassis.

The BigIron series features a range of integrated services modules, including 1-gigabit fiber and 10/100/1000BaseT modules. For data and voice applications, users can connect to the LAN using the 10/100/1000BaseT Ethernet interface on the access devices. The BigIron series is certified in the distribution and access layers when deployed as a component in an ASVALAN or VALAN. The BigIron series was tested for 100 Mbps data load throughput. The BigIron series met all IPv4 and IPv6 requirements. Support for IPv6 is limited to 50,000 packets per second throughput, total of all aggregates, with the Access Control List (ACL) enabled. With the ACL disabled, it met all IPv6 requirements without limitation. The ACL must remain enabled if the BigIron series is used as an access layer device. Currently, there is no defined minimum requirement for packets per second.

The FastIron SX series delivers scalable performance and port density across two chassis configurations. The FastIron SX series is available in an 8- or 16-slot chassis. The FastIron SX series features a range of integrated services modules, including 10-gigabit fiber, 1-gigabit fiber, and 10/100/1000BaseT modules. For data and voice applications, users can connect to the LAN using the 10/100/1000 BaseT Ethernet interface on the access devices. The FastIron SX series provides QoS and ACL capabilities for control of data entering the network. The FastIron SX series is certified in the access layer when deployed as a component in an ASVALAN or VALAN. The FastIron SX series was tested for 100/1000/10000 Mbps data load throughput. The FastIron SX series met all IPv4 and IPv6 requirements.

The FastIron Edge X series delivers performance and port density across four factory configured standalone units. The FastIron Edge X series is available in a model X424-PoE, X424, X424HF, and X448 standalone units. The FastIron Edge X series features a range of factory installed services interfaces, including 1-gigabit fiber, and 10/100/1000BaseT interfaces. Foundry offers a 10 gigabit fiber interface however it was not tested and is not covered under this certification. For data and voice applications, users can connect to the LAN using the 10/100/1000BaseT Ethernet interface on these access devices. The FastIron Edge X series provides QoS and ACL capabilities for control of data entering into the network. The FastIron Edge X series is certified in the access layer when deployed as a component in an ASVALAN or VALAN. The FastIron Edge X series was tested for 100/1000 Mbps data load throughput. The FastIron Edge X series met all IPv4 and IPv6 requirements.

The FastIron GS/LS series delivers performance and port density across four factory configured standalone units. The FastIron GS/LS series is available in a model GS 648P-PoE, GS 624P-PoE, LS 648, and LS 624 standalone units. The FastIron GS/LS series features a range of factory installed services interfaces, including 1-gigabit fiber, and 10/100/1000BaseT interfaces. Foundry offers a 10-gigabit fiber interface however it was not tested and is not covered under this certification. For data and voice applications, users can connect to the LAN using the 10/100/1000 BaseT Ethernet interface on these access devices. The FastIron GS/LS series provides QoS and ACL capabilities for control of data entering into the network. The FastIron GS/LS series is certified in the access layer when deployed as a component in an ASVALAN or VALAN.

The FastIron GS/LS series was tested for 100/1000 Mbps data load throughput. The FastIron GS/LS series met all IPv4 and IPv6 requirements.

The FastIron Edge series delivers performance and port density across two factory configured standalone units. The FastIron Edge series is available in a model 2402-Power over Ethernet (PoE) and 4802-PoE standalone units. The FastIron Edge series features a range of factory installed services interfaces, including 1-gigabit fiber and 10/100BaseT interfaces. For data and voice applications, users can connect to the LAN using the 10/100BaseT Ethernet interface on these access devices. The FastIron Edge series provides QoS and ACL capabilities for control of packets entering into the network. The FastIron Edge series is certified in the access layer when deployed as a component in an ASVALAN or VALAN. The FastIron Edge series was tested for 100 Mbps data load throughput. The FastIron Edge series met all IPv4 and IPv6 requirements. Support for IPv6 is limited to 50,000 packets per second throughput, total of all aggregates, with the ACL enabled. Since the FastIron Edge series is certified just for the access layer, the ACL must remain enabled. Currently, there is no defined minimum requirement for packets per second.

a. Core: The following switches are certified in the core layer when deployed as a component in an ASVALAN or VALAN: NetIron XMR 4000, NetIron XMR 8000, NetIron XMR 16000,NetIron XMR 32000, NetIron MLX 4, NetIron MLX 8, NetIron MLX 16 and NetIron MLX 32.

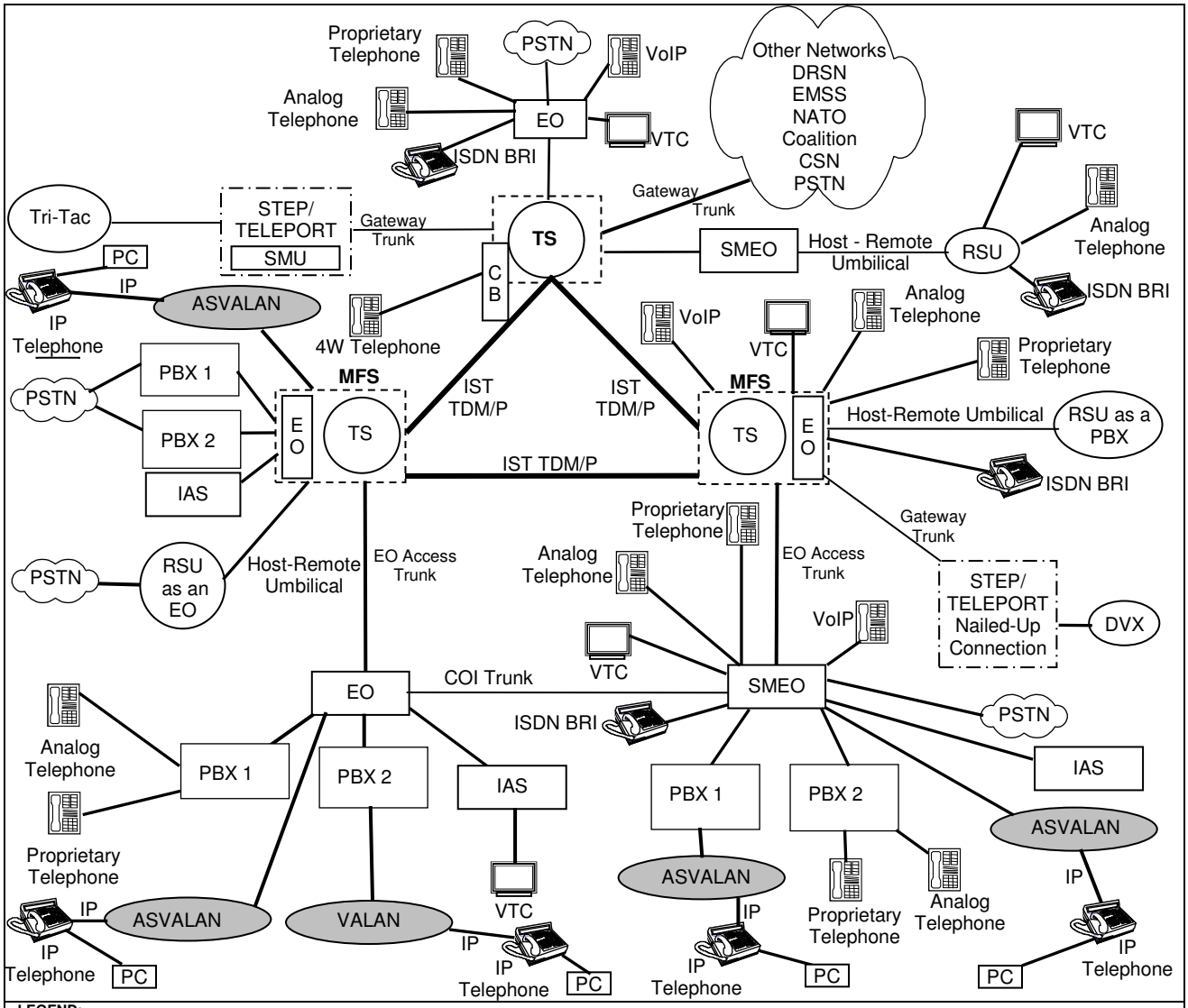
b. Distribution: The following switches are certified in the distribution layer when deployed as a component in an ASVALAN or VALAN: NetIron XMR 4000, NetIron XMR 8000, NetIron XMR 16000, and NetIron XMR 32000, NetIron MLX 4, NetIron MLX 8, NetIron MLX 16, NetIron MLX 32, BigIron RX 4, BigIron RX 8, BigIron RX 16, BigIron RX 32, Foundry BigIron 4000, Foundry BigIron 8000, Foundry BigIron 15000.

c. Access: The following switches are certified in the access layer when deployed as a component in an ASVALAN or VALAN: NetIron XMR 4000, NetIron XMR 8000, NetIron XMR 16000, and NetIron XMR 32000, NetIron MLX 4, NetIron MLX 8, NetIron MLX 16, NetIron MLX 32, BigIron RX 4, BigIron RX 8, BigIron RX 16, BigIron RX 32, Foundry BigIron 4000, Foundry BigIron 8000, Foundry BigIron 15000, FastIron SX 800, FastIron SX 1600, FastIron FESX424-PoE, FastIron FESX424, FastIron FESX424HF, FastIron FESX448, FastIron GS648P-PoE, FastIron GS624P-PoE, FastIron LS648, FastIron LS624, FastIron Edge 4802-PoE, FastIron 2402-PoE.

d. Shared access: Shared access [i.e., same switch port is shared by Personal Computer and IP phone], was tested and is certified with this configuration for 10/100/1000 BaseT. To test 100 Mbps shared access, the IP phones were connected to the 100 Mbps full duplex access switch port and data was generated on the 100 Mbps full duplex Ethernet port on the back of the phones using an IXIA test set. In addition, the NetIron XMR, NetIron MLX, BigIron RX, FastIron SX, FastIron Edge X and the FastIron GS were tested for 1000 Mbps shared access using the IXIA test equipment to simulate shared access traffic of both data and voice packets

simultaneously. This traffic was mapped to a 1 gigabit port to the distribution layer along with other traffic from the IXIA test set to saturate the gigabit port. Voice packets were properly queued by the SUT. All switches that provide Ethernet access ports in this certification were tested for shared access with no measurable degradation of voice traffic.

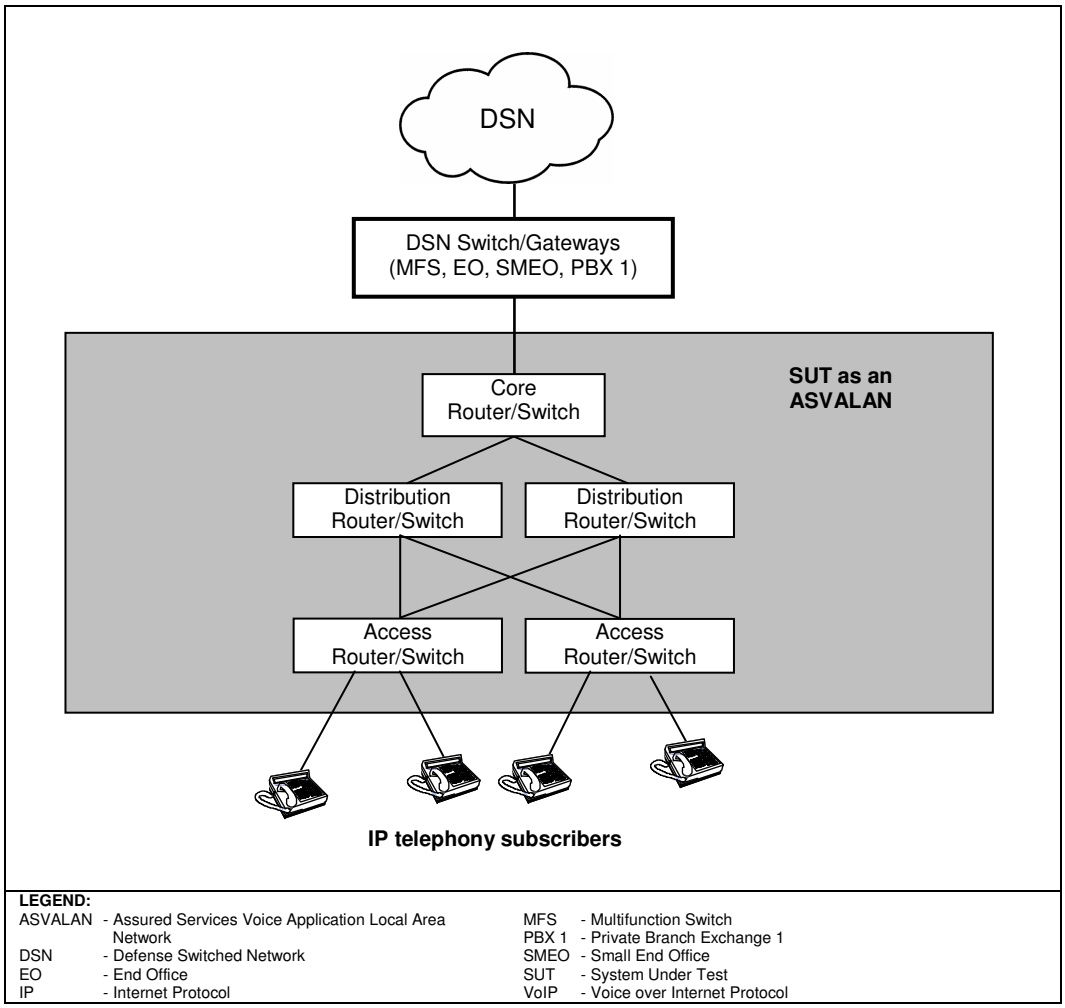
6. OPERATIONAL ARCHITECTURE. The DSN architecture is a two-level network hierarchy consisting of DSN backbone switches and Service/Agency installation switches. Service/Agency installation switches have been authorized to extend voice services over IP infrastructures. The Generic Switching Center Requirements (GSCR) operational DSN Architecture is depicted in figure 2-1, which depicts the relationship of the ASVALAN and VALAN to the DSN switch types. The installation ASVALAN VoIP architecture is depicted in figure 2-2 and VALAN VoIP architecture is depicted in figure 2-3. The ASVALAN and VALAN combined VoIP architecture is depicted in figure 2-4.



LEGEND:

4W	- 4-Wire
ASVALAN	- Assured Services Voice Application Local Area Network
BRI	- Basic Rate Interface
CB	- Channel Bank
COI	- Community of Interest
CSN	- Canadian Switch Network
DRSN	- Defense Red Switch Network
DSN	- Defense Switched Network
DVX	- Deployable Voice Exchange
EMSS	- Enhanced Mobile Satellite System
EO	- End Office
IAS	- Integrated Access Switch
IP	- Internet Protocol
ISDN	- Integrated Services Digital Network
IST	- Interswitch Trunk
MFS	- Multifunction Switch
NATO	- North Atlantic Treaty Organization
PBX	- Private Branch Exchange
PBX 1	- Private Branch Exchange 1
PBX 2	- Private Branch Exchange 2
PC	- Personal Computer
PSTN	- Public Switched Telephone Network
RSU	- Remote Switching Unit
SMEO	- Small End Office
SMU	- Switched Multiplex Unit
STEP	- Standardized Tactical Entry Point
TDM/P	- Time Division Multiplex/Packetized
Tri-Tac	- Tri-Service Tactical Communications Program
TS	- Tandem Switch
VALAN	- Voice Application Local Area Network
VoIP	- Voice over Internet Protocol
VTC	- Video Teleconferencing
	- System Under Test

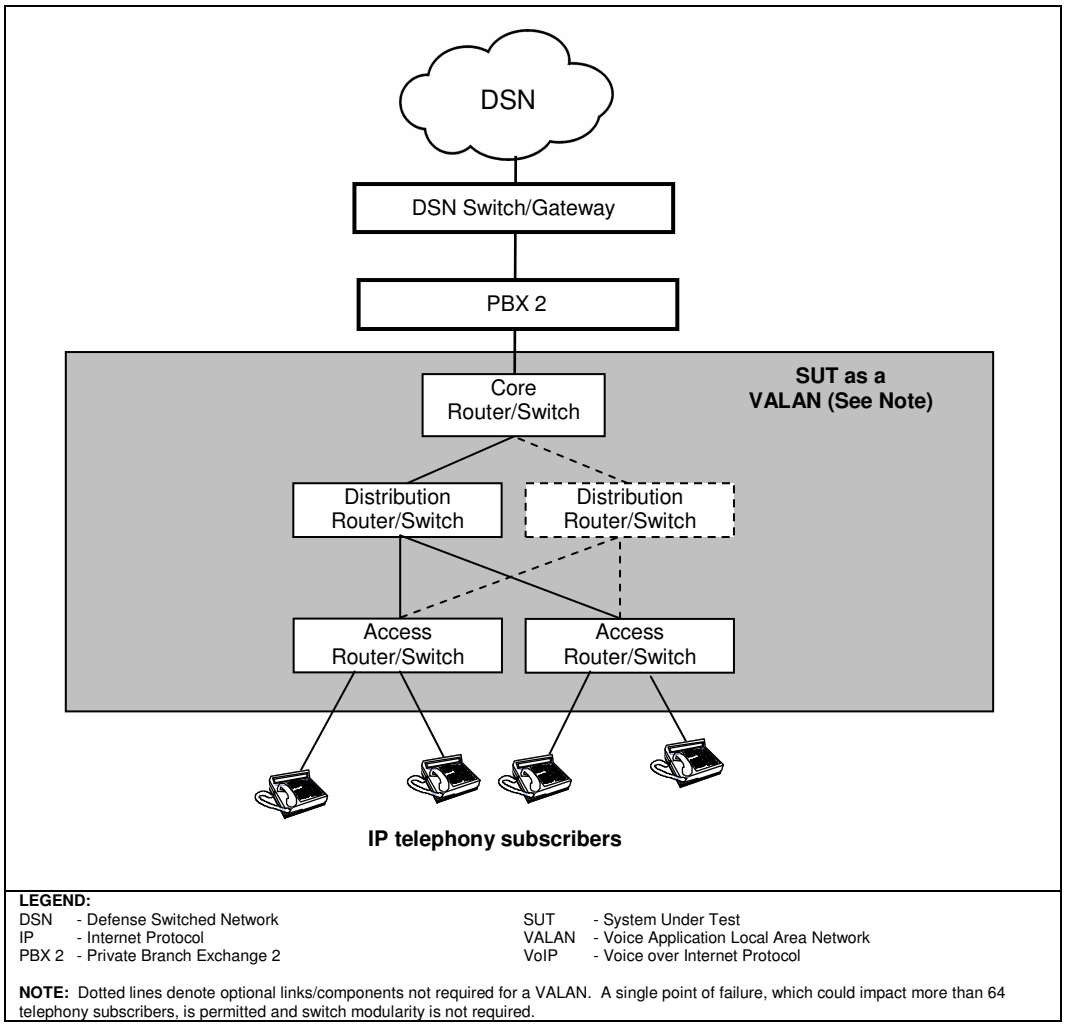
Figure 2-1. DSN Architecture



LEGEND:

ASVALAN	- Assured Services Voice Application Local Area Network	MFS	- Multifunction Switch
DSN	- Defense Switched Network	PBX 1	- Private Branch Exchange 1
EO	- End Office	SMEO	- Small End Office
IP	- Internet Protocol	SUT	- System Under Test
		VoIP	- Voice over Internet Protocol

Figure 2-2. ASVALAN VoIP Architecture

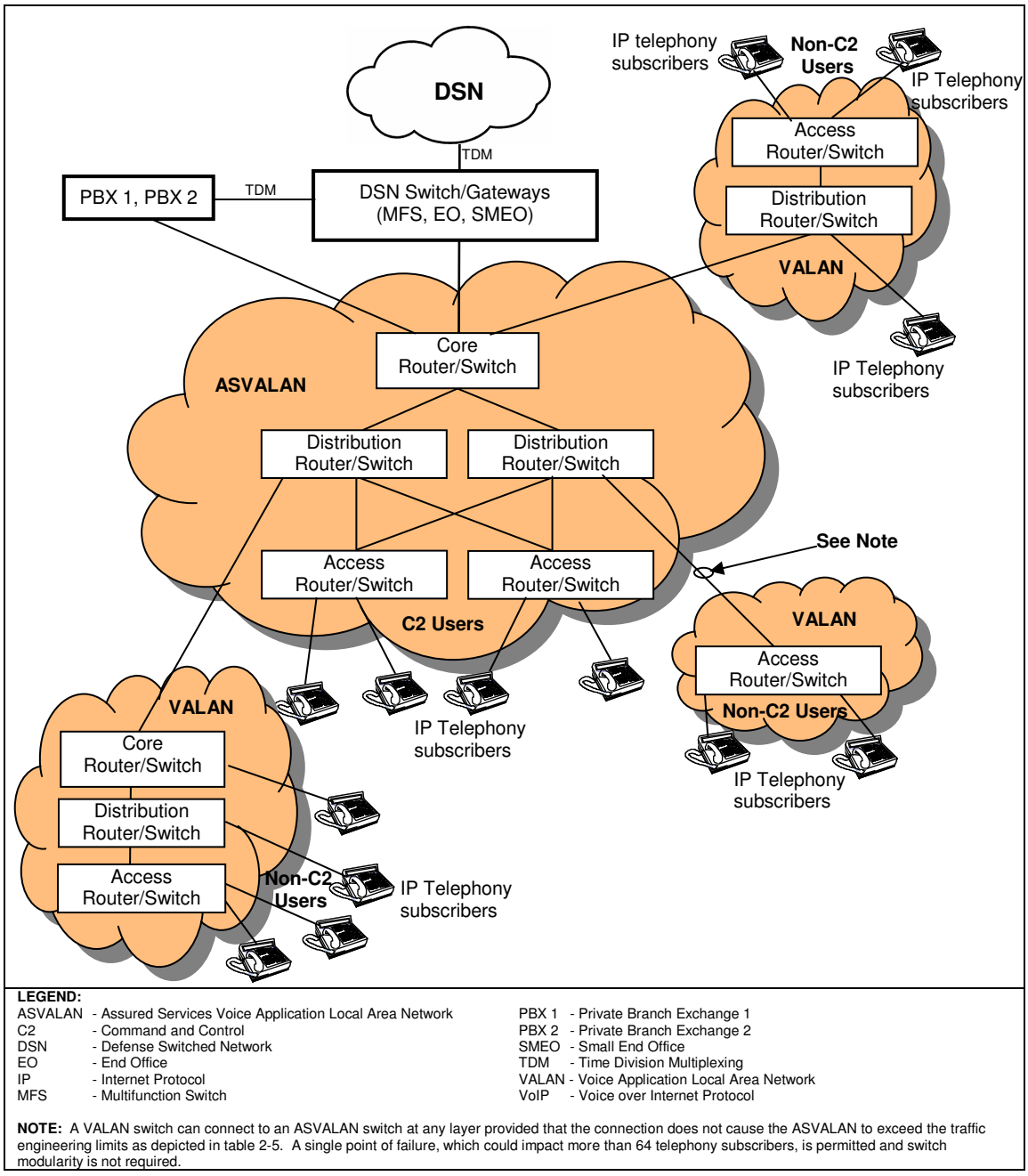


LEGEND:

DSN	- Defense Switched Network	SUT	- System Under Test
IP	- Internet Protocol	VALAN	- Voice Application Local Area Network
PBX 2	- Private Branch Exchange 2	VoIP	- Voice over Internet Protocol

NOTE: Dotted lines denote optional links/components not required for a VALAN. A single point of failure, which could impact more than 64 telephony subscribers, is permitted and switch modularity is not required.

Figure 2-3. VALAN VoIP Architecture



LEGEND:

ASVALAN	- Assured Services Voice Application Local Area Network	PBX 1	- Private Branch Exchange 1
C2	- Command and Control	PBX 2	- Private Branch Exchange 2
DSN	- Defense Switched Network	SMEO	- Small End Office
EO	- End Office	TDM	- Time Division Multiplexing
IP	- Internet Protocol	VALAN	- Voice Application Local Area Network
MFS	- Multifunction Switch	VoIP	- Voice over Internet Protocol

NOTE: A VALAN switch can connect to an ASVALAN switch at any layer provided that the connection does not cause the ASVALAN to exceed the traffic engineering limits as depicted in table 2-5. A single point of failure, which could impact more than 64 telephony subscribers, is permitted and switch modularity is not required.

Figure 2-4. ASVALAN and VALAN Combined VoIP Architecture

7. REQUIRED SYSTEM INTERFACES. The SUT ASVALAN and VALAN system requirements are listed in table 2-1. The requirements specific to the SUT ASVALAN and VALAN components are shown in table 2-2. These requirements are derived from:

a. DSN services for Network and Applications specified in Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6215.01B, "Policy for Department of Defense Voice Services."

b. GSCR, appendix 3, Capability Requirements (CRs) and Feature Requirements (FRs) verified through JITC testing and/or vendor submission of Letters of Compliance (LoC).

Table 2-1. ASVALAN and VALAN System Requirements

System Requirements				
Requirement	**Criteria**		**Reference**	**Required**
Delay	One-way packet delay for voice packets of an established call (signaling and media) shall be 5 ms or less averaged over any 5-minute period.		GSCR, Appendix 3, paragraph A.3.3.1.1	Yes
Jitter	For voice media packets, jitter shall be 5 ms or less averaged over any 5-minute period.		GSCR, Appendix 3, paragraph A.3.3.1.2	Yes
Packet Loss	Voice packet loss within the LAN shall not exceed 0.05% averaged over any 5-minute period.		GSCR, Appendix 3, paragraph A.3.3.1.3	Yes
Reliability	ASVALAN	- ASVALANs shall have a reliability of .99999 - No single point of failure for outage of more than 64 telephony subscribers - Network Path restores within 2 seconds	GSCR, Appendix 3, paragraph A.3.3.4.1	Yes
	VALAN	- This requirement is conditional for a VALAN.	GSCR, Appendix 3, paragraph A.3.3.4.1	No
IPv6[1]	All IP devices shall be IPv6 capable.		GSCR paragraph 1.7, and GSCR, Appendix 3, paragraph A3.2.8	Yes
Security[2]	DIACAP (replacement for DITSCAP)/IA		GSCR, Appendix 3, paragraph A.3.3.4.3	Yes

LEGEND:

ASVALAN	- Assured Services Voice Application LAN	IP	- Internet Protocol
DIACAP	- DoD IA Certification and Accreditation Process	IPv4	- Internet Protocol version 4
DISA	- Defense Information Systems Agency	IPv6	- Internet Protocol version 6
DITSCAP	- DoD IT Security Certification and Accreditation Process	IT	- Information Technology
DoD	- Department of Defense	LAN	- Local Area Network
GSCR	- Generic Switching Center Requirements	ms	- milliseconds
IA	- Information Assurance	VALAN	- Voice Application LAN

NOTES:

1 An IPv6 capable system or product, as defined in the GSCR, paragraph 1.7, shall be capable of receiving, processing, and forwarding IPv6 packets and/or interfacing with other systems and protocols in a manner similar to that of IPv4. IPv6 capability is currently satisfied by a vendor Letter of Compliance signed by the Vice President of the company. The vendor must state, in writing, compliance to the following criteria**:**
   a. Conformant with IPv6 standards profile contained in the DoD IT Standards Registry (DISR).
   b. Maintaining interoperability in heterogeneous environments and with IPv4.
   c. Commitment to upgrade as the IPv6 standard evolves.
   d. Availability of contractor/vendor IPv6 technical support.

2 Security testing is accomplished via DISA-led Information Assurance test teams and published in a separate report.

Table 2-2. ASVALAN and VALAN Component Requirements

Core/Distribution/Access Component Requirements				
Requirement	**Criteria**		**Reference**	**Required**
CoS Models	LAN components shall support IEEE 802.1p to DSCP mapping and at least one of the following: - IEEE 802.1p/Q priority tagging/VLAN tagging - DSCP - ToS		GSCR, Appendix 3, paragraph A.3.3.2.1	Yes
Traffic Prioritization	Traffic within LAN components shall be prioritized so that voice signaling receives highest priority, voice media second highest priority, and data lowest priority.		GSCR, Appendix 3, paragraph A.3.3.2.2	Yes
QoS	LAN components shall support one of the following: - Priority Queuing - Custom Queuing - Weighted Fair Queuing - Class Based Weighted Fair Queuing		GSCR, Appendix 3, paragraph A.3.3.3.1	Yes
Policing	LAN components shall support one of the following: - DSCP PHB - Generic Traffic Shaping - Class-Based Shaping		GSCR, Appendix 3, paragraph A.3.3.3.2	Yes
VLANs	LAN components shall support: - Port based VLANs - MAC address based VLANs - Protocol based VLANs		GSCR, Appendix 3, paragraph A.3.3.3.3	Yes
IEEE Conformance	LAN components shall support: - IEEE 802.1d – Bridging - IEEE 802.1p/Q – Priority tagging/VLAN tagging - IEEE 802.1s – Per-VLAN Group Spanning Tree - IEEE 802.1v – VLAN Classification by port and protocol - IEEE 802.1w –Rapid Reconfiguration of Spanning Tree - IEEE 802.1x – Port Based Network Access Control - IEEE 802.3ad – Link Aggregation Protocol		GSCR, Appendix 3, paragraph A.3.3.4	Yes
Reliability	ASVALAN	LAN components shall support: - ASVALAN components shall have a reliability of .99999 or better - Dual power supplies and dual processors (more than 64 telephony subscribers) - N+1 sparing for access (more than 64 telephony subscribers) - Redundancy protocol[1] - 2 second path restoral	GSCR, Appendix 3, paragraph A.3.3.4.1	Yes
	VALAN	This requirement is conditional for a VALAN.	GSCR, Appendix 3, paragraph A.3.3.4.1	No
Network Management	ASVALAN	LAN components shall support: - In-band or out-of-band management - SNMP - Measurements	GSCR, Appendix 3, paragraph A.3.3.4.2	Yes
	VALAN	This requirement is conditional for a VALAN.	GSCR, Appendix 3, paragraph A.3.3.4.2	No
Security	LAN components shall employ the Network Infrastructure and VoIP STIGs.[2]		GSCR, Appendix 3, paragraph A.3.3.4.3	Yes
IPv6	All IP devices shall be IPv6 capable.[3]		GSCR paragraph 1.7, and GSCR, Appendix 3, paragraph A3.2.8	Yes
TE	ASVALAN	- ASVALAN components shall be engineered for a maximum of 25% voice traffic per link.[4] - For more than 64 telephony subscribers, link pairs (redundant links) must be used.	GSCR, Appendix 3, paragraph A.3.3.4.4	Yes
	VALAN	VALAN components shall be engineered for a maximum of 25% voice traffic per link.[4]	GSCR, Appendix 3, paragraph A.3.3.4.4	Yes

Table 2-2. ASVALAN and VALAN Component Requirements (continued)

LEGEND:

802.1d	- Standard for Local and Metropolitan Area Networks: MAC Bridges
802.1p	- LAN Layer 2 QoS/CoS Protocol for Traffic Prioritization
802.1Q	- Standards for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks
802.1s	- Standard for Local and Metropolitan Area Networks - Amendment 3 to 802.1Q Virtual Bridged Local Area Networks: Multiple Spanning Trees
802.1v	- Standard for Local and Metropolitan Area Networks - Virtual Bridge Local Area Networks - Amendment 2: VLAN Classification by Protocol and Port (Amendment to IEEE 802.1Q, 1998 Edition)
802.1w	- Standard for Local and metropolitan area networks - Common Specifications - Part 3: Media Access Control (MAC) Bridges: Rapid Configuration
802.1x	- Standard for Local and Metropolitan Area Networks Port-Based Network Access Control
802.3ad	- Standard for Information Technology – Local and Metropolitan Area Networks – Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications–Aggregation of Multiple Link Segments
ASVALAN	- Assured Services Voice Application LAN
CoS	- Class of Service
DISA	- Defense Information Systems Agency
DSCP	- Differentiated Services Code Point
GSCR	- Generic Switching Center Requirements
IEEE	- Institute of Electrical and Electronics Engineers, Inc.
IP	- Internet Protocol
IPv4	- Internet Protocol version 4
IPv6	- Internet Protocol version 6
LAN	- Local Area Network
MAC	- Media Access Control
Mbps	- Megabits per second
N	- total VoIP users / 64
OSPFV.3	- Open Shortest-Path First Version 3
PHB	- Per Hop Behaviors
QoS	- Quality of Service
SNMP	- Simple Network Management Protocol
STIGs	- Security Technical Implementation Guides
TE	- Traffic Engineering
ToS	- Type of Service
VALAN	- Voice Application LAN
VLANs	- Virtual LANs
VoIP	- Voice over Internet Protocol
VRRP	- Virtual Router Redundancy Protocol

NOTES:

1 For core and distribution components, OSPFV.3 redundancy protocol shall be the routing protocol supported. For access components, redundancy protocol shall be VRRP or equivalent protocol.

2 Verified using the Information Assurance Test Plan. Results of the security testing are published in a separate test report generated by the DISA Information Assurance test personnel.

3 An IPv6 capable system or product, as defined in the GSCR, paragraph 1.7, shall be capable of receiving, processing, and forwarding IPv6 packets and/or interfacing with other systems and protocols in a manner similar to that of IPv4. IPv6 capability is currently satisfied by a vendor Letter of Compliance signed by the Vice President of the company. The vendor must state, in writing, compliance to the following criteria:
   a. Conformant with IPv6 standards profile contained in the Department of Defense Information Technology Standards Registry (DISR).
   b. Maintaining interoperability in heterogeneous environments and with IPv4.
   c. Commitment to upgrade as the IPv6 standard evolves.
   d. Availability of contractor/vendor IPv6 technical support.

4 Instruments connected to an access device must provide a minimum of a 10 Mbps full duplex link. For core and distribution connections, the minimum link capacity is 100 Mbps full duplex.

8. TEST NETWORK DESCRIPTION. The SUT was tested at JITC's Global Information Grid Network Test Facility in a manner and configuration similar to that of the DSN operational environment. Figure 2-5 depicts the SUT test configuration.

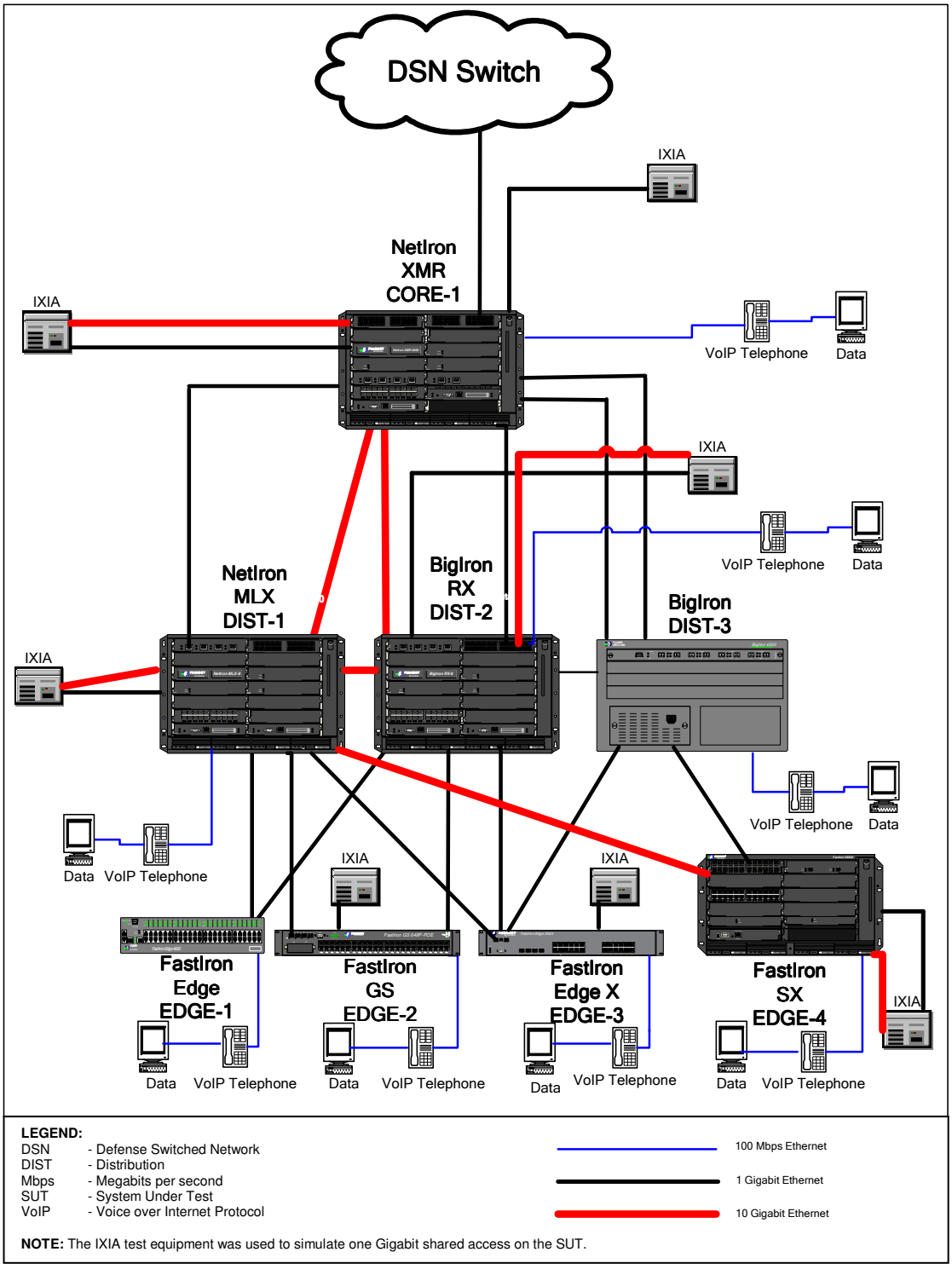


Figure 2-5. SUT Test Configuration

9. SYSTEM CONFIGURATIONS. Table 2-3 provides the system configurations, hardware and software components tested with the SUT. The SUT was tested in an operationally realistic environment to determine interoperability with the DSN switch noted in table 2-3. The DSN switch listed in table 2-3 only depicts the tested configuration. Table 2-3 is not intended to identify the only switches that are certified with the SUT. The SUT is certified with switching systems listed on the DSN Approved Products List (APL) that are certified for use with an ASVALAN or VALAN.

Table 2-3. Tested System Configurations

System Name	**Software Release**		
Avaya S8500	Communication Manager (CM) 4.0 (R014x.00.2.731.7: Super Patch 14419)		
System Under Test Components with Current Operating System			
Component (See note.)	**Release**	**Sub-component** (See note.)	**Function**
Foundry NetIron XMR 4000/**8000**/16000/ 32000	3.3.0e	**NI-XMR-MR**	Core Processor for 4000/8000/16000 system
		NI-XMR-32-MR	Core Processor for 32000 system
		NI-X-SF1	Switch Fabric for 4000 system
		NI-X-SF3	Switch Fabric for 8000/16000 system
		NI-X-32-SF	Switch Fabric for 32000 system
		NI-XMR-10Gx2	2 Port 1/10 Gig fiber module
		NI-XMR-10Gx4	4 Port 1/10 Gig fiber module
		NI-XMR-1Gx20-SFP	20-Port 1 Gig fiber module
		NI-XMR-1Gx20-GC	20-Port 10/100/1000 Mbps copper module
Foundry NetIron MLX 4/**8**/16/32	3.3.0e	**NI-MLX-MR**	Core Processor for 4/8/16 system
		NI-MLX-32-MR	Core Processor for 32 system
		NI-X-SF1	Switch Fabric 4 system
		NI-X-SF3	Switch Fabric 8/16 system
		NI-X-32-SF	Switch Fabric 32 system
		NI-MLX-10Gx2	2 Port 1/10 Gig fiber module
		NI-MLX-10Gx4	4 Port 1/10 Gig fiber module
		NI-MLX-1Gx20-SFP	20-Port 1 Gig fiber module
		NI-MLX-1Gx20-GC	20-Port 10/100/1000 Mbps copper module
Foundry BigIron RX 4/**8**/16/32	2.3.0e	**RX-BI-MR**	Core Processor with 512MB Memory
		RX-BI-MR2	Core Processor with 2GB Memory
		RX-BI-32-MR	Core Processor with 512MB Memory for RX-32
		RX-BI-32-MR2	Core Processor with 2GB Memory for RX-32
		RX-BI-SFM1	Switch Fabric for RX-4
		RX-BI-SFM3	Switch Fabric for RX-8 and RX-16
		RX-BI-32-SFM	Switch Fabric for RX-32
		RX-BI-BI2XG	2 Port 1/10 Gig fiber module
		RX-BI-BI4XG	4 Port 1/10 Gig fiber module
		RX-BI-BI24F	24-Port Gig Ethernet SFP module
		RX-BI-BI24HF	24-Port 100/1000 Ethernet SFP module
		RX-BI-BI24C	24-Port 10/100/1000 Mbps copper module
Foundry BigIron 4000/8000/ 15000	8.0.01k	**J-BxGMR4**	Core Processor with 8 port 1 Gig module
		J-B2GMR4	Core Processor with 2 port 1 Gig module
		J-BxG	8-Port mini-GBIC based Gig module
		J-B16Gx	16-Port mini-GBIC based Gig module
		J-B16GC	24-Port 10/100 Mbps Base-T copper module
		J-B48E	48-Port 10/100 Mbps RJ-45 copper module
		J-B48T	48-Port 10/100 Mbps RJ-21 copper module

Table 2-3. Tested System Configurations (continued)

Component (See note.)	Release	Sub-component (See note.)	Function
FastIron SX 800/SX 1600	3.3.00	**SX-FIZMR**	Core Processor SX-800 and SX-1600
		FI-FISF	Switch Fabric SX-800 and SX-1600
		SX-FI42XG	2 Port XFP 10 Gig Ethernet module
		SX-FI42XGW	2 Port LAN/WAN XFP 10 Gig Ethernet module
		SX-FI424F	24-Port mini-GBIC based Ethernet module
		SX-FI424C	24-Port 10/100/1000 Ethernet module
		SX-FI424HF	24-Port 10/100/1000 Combo Fiber Ethernet module
		SX-FI424P	24-Port 10/100/1000 Ethernet module with PoE
FastIron FESX424-PoE/ FESX424/FESX4 24HF/ FESX448	3.3.00	Not Applicable	4-port T/X interface and 20-P10/100/1000 Mbps copper interface
FastIron GS648P-PoE GS624P-PoE/LS648/LS624	3.2.00	Not Applicable	4-port T/X interface and 44-P10/100/1000 Mbps interface
FastIron Edge 4802-PoE/2402-PoE	3.7.00a	Not Applicable	2-port T/X interface and 48-P 10/100 Mbps copper interface

LEGEND:

10BaseT	- 10 Mbps (Baseband Operation, Twisted Pair) Ethernet	LAN	- Local Area Network
100BaseT	- 100 Mbps (Baseband Operation, Twisted Pair) Ethernet	MB	- Megabyte
1000BaseT	- 1000 Mbps (Baseband Operation, Twisted Pair) Ethernet	Mbps	- Megabits per second
GB	- Gigabyte	PoE	- Power over Ethernet
GBIC	- Gigabit Interface Card	RJ	- Registered Jack
Gig	- Gigabit	SFP	- Smal Form Factor Pluggable
JITC	- Joint Interoperability Test Command	WAN	- Wide Area Network

NOTE: Components and sub-components bolded and underlined were tested by JITC. The other components in the family series were not tested; however, they utilize the same Operating software and hardware and JITC analysis determined them to be functionally identical for interoperability certification purposes and they are also certified for joint use.

10. TESTING LIMITATIONS. None.

11. TEST RESULTS

a. Components. The SUT met the minimum interoperability requirements of the GSCR, appendix 3, for an ASVALAN. If a system meets the minimum requirements for an ASVALAN, it also meets the lesser requirements for a VALAN. The network consisted of three main components: core switches, distribution switches, and access switches. The test results are provided below.

(1) Class of Service (CoS). The GSCR, appendix 3, section A3.3.2, outlines several methodologies to implement CoS. The SUT employed Institute of Electrical and Electronics Engineers, Inc. (IEEE) 802.1p/Q at the Data Link Layer (L2) and Differentiated Services Code Point (DSCP) at the Network Layer (L3) and 802.1p/Q to DSCP mapping, which was verified by capturing packets at both layers within the network.

(2) Traffic Prioritization. Priorities were applied in accordance with the CoS listed above. This ensured voice signaling would get the highest level of priority; voice media stream would be prioritized lower than voice signaling but higher than data, and data traffic would receive the lowest priority. At L2, packets were tagged as: Data

traffic = 0, Voice media = 5 and Voice Signaling and Network Management = 6, for L3 prioritization, DSCP were marked 0, 46, and 48 respectively. By filling uplinks to their capacity with data packets tagged at 0, we were able in inject voice packets, tagged with 46 for voice media and 48 for voice signaling to ensure they received treatment in a higher queue and were not delayed throughout the network. Trust DSCP and trust CoS statements were applied between all ports. By filling uplinks to their capacity with data packets tagged at 0, we were able in inject voice packets, tagged with 5 and 6 and ensure they received precedence and were not delayed.

In addition, flooding parameters were set to prevent broadcast and multicast traffic from overwhelming the ports. Broadcast limits were set to no greater then 10% and multicast limits were set to a max of 10%. The configuration changes that were made to ensure proper operation can be found on the Telecom Switched Services Interoperability (TSSI) website at http://jitc.fhu.disa.mil/tssi.

(3) QoS. Foundry's QoS process is supported by 8 queues uses Weighted Fair Queuing. Packets tagged with a CoS of 6 are queued in a highest priority queue. The CoS values of 5 and 0 are placed in separate queues, with 5 receiving a higher value therefore, it will be serviced more frequently then 0. These tags were used to identify and separate traffic types that pass through the network connections ensuring that signaling traffic and voice traffic take precedence over data traffic.

(4) Policing. The SUT implemented Class Based Weighted Fair Queuing that uses DSCP values to define how traffic is treated at each individual network node. DSCP values are used from the L3 IP header.

(a) Queuing. The GSCR, appendix 3, paragraph 3.3.3.1, outlines that an ASVALAN must support at least one of the following queuing mechanisms: Priority Queuing, Custom Queuing, Weighted Fair Queuing, or Class-Based Weighted Fair Queuing. The SUT supports a Class-Based Weighted Fair Queuing as required in the GSCR. Traffic classes are weighted based on criteria including ACLs, protocols, and QoS labels. Packets meeting the criteria for a class make up the traffic for that class. A queue is reserved for each of the classes, and traffic belonging to a given class is directed to the queue for that class. Classes are assigned: bandwidth, weight, and maximum packet limit. Bandwidth assigned to any class is guaranteed for that class during times of congestion. Each class has the queue limit assigned and is the maximum amount of packets that can accumulate in the queue for the class. Packets belonging to a class are subject to bandwidth and queue limits for the class. After a queue has reached its queue limit, queuing of additional packets to the class causes packet to be dropped.

L2 packets tagged with a CoS of 6 are queued in the highest priority queue. The CoS values 5 and 0 are serviced in separate queues, with 5 receiving a higher value therefore, it will be serviced more frequently then 0. These tags were used to identify and separate traffic types as it passed through network connections ensuring voice traffic takes precedence over data traffic.

(b) Policing. Traffic Policing limits the input or output transmission rate of a class of traffic based on user-defined criteria and marks packets by setting the IP Precedence value, the QoS group, or the DSCP value. The GSCR, appendix 3, paragraph A3.3.3.2, outlines that the ASVALAN must meet at least one of the following policing mechanisms: DiffServ Per-Hop Behavior (PHB), Generic Traffic Shaping (GTS), or Class-Based Shaping (CBS). The SUT implemented CBS that uses DSCP values to define how traffic is treated at each individual network node. DSCP values are used from the L3 IP header. CBS shapes traffic exiting an interface and matches its speed to the distant end interface. Based on class, CBS specifies the average rate or peak rate, reduces output flow to avoid bottlenecks and ensures traffic conforms to policies setup for it. CBS uses Class-Based Weighted Fair Queuing.

(4) Virtual LAN (VLAN). The GSCR, appendix 3, paragraph A3.3.3.3 outlines that the ASVALAN shall support either implicit or explicit VLAN membership for: Port-based VLANs, Media Access Control (MAC) address-based VLANs, or Layer 3 protocol-based VLANs. The SUT supports port-based VLANs. Switches within the topology were configured with multiple VLANs using the IEEE 802.1Q tag to separate data from voice traffic. MAC address and Protocol-based VLANs were verified through the LoC as well as packet captures.

(5) IEEE Conformance. All aspects of IEEE conformance were met through the LoC or testing. All test results are discussed under their respective topics.

(6) Reliability. The GSCR, appendix 3, section A3.3.4.1, requires that there be no single point of failure within the ASVALAN that can cause an outage of more than 64 telephony subscribers. In order to meet the availability requirement of an ASVALAN, all switching/routing platforms that offer more than 64 telephony subscribers shall have a switch design or configuration that provides at a minimum dual power supplies, dual processors, redundancy protocol, and switch fabric redundancy. To meet this requirement, dual Gigabit and/or 10 Gigabit Routed Links (RL) were configured between the core and distribution switches, and dual Gigabit and/or 10 Gigabit layer 2 rapid spanning tree links connected the Distribution and Access switches, as shown in figure 2-5. The dual RLs from the distribution to the core must be terminated onto separate fiber cards at the core switch. Reliability is a conditional requirement for a VALAN.

(7) Network Management. The GSCR, appendix 3, paragraph A3.3.4.2, requires that the vendor provide a management system to monitor the performance of the ASVALAN portion of the VoIP system. Due to numerous third party systems and applications capable of performing this function, this requirement was verified via LoC. Network Management features are conditional requirements for a VALAN.

(8) Security. Security requirements in accordance with the GSCR, appendix 3, paragraph A3.3.4.3, were verified using the Information Assurance Test Plan. Results of the security testing are reported in a separate test report generated by the Defense Information Systems Agency (DISA) Information Assurance test personnel.

(9) Internet Protocol version 6 (IPv6). An IPv6 capable system or product, as defined in the GSCR, paragraph 1.7, shall be capable of receiving, processing, and forwarding IPv6 packets and/or interfacing with other systems and protocols in a manner similar to that of Internet Protocol version 4 (IPv4). IPv6 capability is currently satisfied by testing and a vendor Letter of Compliance signed by the Vice President of the company. The vendor stated, in writing, compliance to the following criteria:

(a) Conformant with IPv6 standards profile contained in the Department of Defense (DoD) Information Technology Standards Registry (DISR).

(b) Maintaining interoperability in heterogeneous environments and with IPv4.

(c) Commitment to upgrade as the IPv6 standard evolves.

(d) Availability of contractor/vendor IPv6 technical support.

Open Shortest-Path First version 2 (OSPF V.2) and Open Shortest-Path First version three (OSPF V.3) were used during the tests. OSPF V.2 was required for IPv4 compatibility and OSPF V.3 was required for IPv6 compatibility. All of the SUT components covered under this certification met the IPv6 criteria.

(10) Traffic Engineering

(a) Links. To meet the ASVALAN requirements, all links connected between the core and distribution as shown in figure 2-5, are configured as RLs. To meet the ASVALAN requirements for failover, all links connected between the core and distro and between distro switches were configured as shown in figure 2-5. The two RLs between the core and distro must be terminated on separate fiber cards at each switch.

(b) Scalability. The SUT can be scaled to meet any number of IP phone subscribers as long as the SUT is composed of the equipment and software listed in table 2-3, and are consistent with traffic engineering constraints contained in the GSCR, appendix 3. Table 2-4, which was approved by the DSN Configuration Control Board (DSN CCB) on Dec 2004, outlines the maximum number of subscribers that can be supported per each link capacity.

Table 2-4. IP Subscriber Supportability by Link Capacity

Link Type	LAN BW	Users
Non-Converged	10 Mbps	64 (See note 1.)
	100 Mbps	64 (See note 1.)
	1 Gbps	64 (See note 1.)
	10 Gbps	64 (See note 1.)
	10 Mbps LP	100 (See note 2.)
	100 Mbps LP	1000 (See note 2.)
	1 Gbps LP	10000 (See note 2.)
	10 Gbps LP	100000 (See note 2.)
Converged	10 Mbps	25 (See note 3.)
	100 Mbps	64 (See note 1.)
	1 Gbps	64 (See note 1.)
	10 Gbps	64 (See note 1.)
	10 Mbps LP	25 (See note 3.)
	100 Mbps LP	250 (See note 4.)
	1 Gbps LP	2500 (See note 4.)
	10 Gbps LP	25000 (See note 4.)

LEGEND:

ASVALAN	- Assured Services Voice Application LAN	kbps	- kilobits per second
BW	- Bandwidth	LAN	- Local Area Network
Gbps	- Gigabits per second	LP	- Link Pair
IP	- Internet Protocol	Mbps	- Megabits per second

NOTES:

1 For single links, number of telephony subscribers is limited to a maximum of 64 because of single point of failure. This limit applies specifically to ASVALANs.
2 The number of users is calculated as bandwidth (BW) divided by 100 kbps per user.
3 The number of users was limited to 64 telephony subscribers per note 1 or 25% of total users per note 1, whichever was less.
4 For the converged network, voice traffic was engineered not to exceed 25 % of total utilization using an estimated 100 kbps per voice call.

(11) LAN Architectures. To meet the ASVALAN failover requirements, OSPF V.3 was implemented between the core and distribution layer. OSPF V.3 utilizes link-state protocols to identify lowest cost paths within the LAN. Additionally, OSPF V.3 is an open standard, and would likely be a common protocol between different vendors equipment.

(a) Delay. The GSCR, appendix 3, section A3.3.1.1, states the one-way packet delay shall be five milliseconds (ms) or less, as measured over a five-minute period. The average one-way delay for each of the sampled five-minute periods, measured between the access and core devices, was 0.18 ms, with a maximum delay of 1.0 ms, which met the requirement.

(b) Jitter. The GSCR, appendix 3, section A3.3.1.2 states jitter for voice media packets will be 5 ms or less as averaged over any five-minute period. With a 100% bandwidth load, jitter was measured to be 0.0 ms or less over a five-minute period, which met the requirement.

(c) Packet Loss. Network packet loss occurs when packets are sent, but not received at the final destination. The GSCR, appendix 3, section A3.3.1.3, states that LANs shall be engineered so the measured voice packet loss within the LAN shall not exceed 0.05% averaged over any five-minute period. With 100% bandwidth load, the measured packet loss was 0.00%, which met the requirement.

b. System Interoperability Results. The SUT is certified for joint use within the DSN with the Digital Switching Systems listed on the DSN APL which are certified for use with an ASVALAN or VALAN. The SUT is certified to support DSN assured services over IP as an ASVALAN in accordance with the requirements set forth in the GSCR, appendix 3. The SUT is also certified as a VALAN. However, since VALANs do not support the Assured Services Requirements detailed in reference (c), Command and Control (C2) users and Special C2 users are not authorized to be served by a VALAN. Since VALANs do not support Assured Services, they can only serve DoD, non-DoD, non-governmental, and foreign government users having no missions or communications requirement to ever originate or receive C2 communications. VALAN connectivity to the DSN is not authorized until a waiver is granted by the Joint Staff for each site. The system interoperability test summary is shown in table 2-5 and the detailed component interoperability test status is shown table 2-6.

Table 2-5. SUT System Interoperability Test Summary

Device Requirement[1]	Reference	Test Results	Remarks
Delay measured at 5 ms or less	GSCR, Appendix 3, A3.3.1.1	Met	The average was 0.18 ms and the maximum was 1.0 ms.
Jitter measured at less than 5 ms	GSCR, Appendix 3, A3.3.1.2	Met	Measured to be 0.0 ms or less.
Packet Loss less than 0.05%	GSCR, Appendix 3, A3.3.1.3	Met	Measured to be 0.00%.
Reliability	GSCR, Appendix 3, Section A.3.3.4.1	Met	See note 2.
IPv6	GSCR, Appendix 3, Section A3.2.8	Met	See note 3.
Security	GSCR, Appendix 3, A3.2.4	Met	See note 4.

LEGEND:

ASVALAN	- Assured Services Voice Application Local Area Network	IPv4	- Internet Protocol version 4
DISA	- Defense Information Systems Agency	IPv6	- Internet Protocol version 6
DISR	- DoD Information Technology Standards Registry	ms	- millisecond
DoD	- Department of Defense	SUT	- System Under Test
GSCR	- Generic Switching Center Requirements	VALAN	- Voice Application Local Area Network

NOTES:

1 If a system meets the minimum requirements for an ASVALAN, it also meets the lesser requirements for a VALAN.

2 Reliability is a conditional requirement for a VALAN.

3 An IPv6 capable system or product, as defined in the GSCR, paragraph 1.7, shall be capable of receiving, processing, and forwarding IPv6 packets and/or interfacing with other systems and protocols in a manner similar to that of IPv4. IPv6 capability is currently satisfied by a vendor Letter of Compliance signed by the Vice President of the company. The vendor must state, in writing, compliance to the following criteria:
   a. Conformant with IPv6 standards profile contained in the DISR.
   b. Maintaining interoperability in heterogeneous environments and with IPv4.
   c. Commitment to upgrade as the IPv6 standard evolves.
   d. Availability of contractor/vendor IPv6 technical support.

4 Security is tested by DISA-led Information Assurance test teams and published in a separate report.

Table 2-6. Component Interoperability Test Summary

DSN Line Interfaces						
Interface	**Component**	**Status**	**Device Requirement**	**Test Results**	**Reference**	**Remarks**
1000/10000 BaseFX 10/100/1000 BaseTX	**Foundry NetIron XMR** 4000/**8000**/16000 /32000	Certified as: Core Distribution Access	CoS Models	Met	GSCR, Appendix 3, A3.3.2.1	
			Traffic Prioritization	Met	GSCR, Appendix 3, A3.3.2.2	
			QoS	Met	GSCR, Appendix 3, A3.3.3	
			Policing	Met	GSCR, Appendix 3, A3.3.3.2	
			VLANs	Met	GSCR, Appendix 3, A3.3.3.3	
			IEEE Conformance	Met	GSCR, Appendix 3, A3.3.4	
			Reliability	Met	GSCR, Appendix 3, A3.3.4.1	Reliability is a conditional requirement for a VALAN .[1]
			Network Management	Met	GSCR, Appendix 3, A.3.3.4.2	Network Management Reliability is a conditional requirement for a VALAN .[1]
			Security	Met	GSCR, Appendix 3, A.3.3.4.3	See note 2.
			IPv6	Met	GSCR, Paragraph 1.7, and Appendix 3, A3.2.8	See note 3.
			TE	Met	GSCR, Appendix 3, A.3.3.4.4	For a VALAN, redundant links are not required.[1]
1000/10000 BaseFX 10/100/1000 BaseTX	**Foundry NetIron MLX** 4/**8**/16/32	Certified as: Core, Distribution Access	CoS Models	Met	GSCR, Appendix 3, A3.3.2.1	
			Traffic Prioritization	Met	GSCR, Appendix 3, A3.3.2.2	
			QoS	Met	GSCR, Appendix 3, A3.3.3	
			Policing	Met	GSCR, Appendix 3, A3.3.3.2	
			VLANs	Met	GSCR, Appendix 3, A3.3.3.3	
			IEEE Conformance	Met	GSCR, Appendix 3, A3.3.4	
			Reliability	Met	GSCR, Appendix 3, A3.3.4.1	Reliability is a conditional requirement for a VALAN .[1]
			Network Management	Met	GSCR, Appendix 3, A.3.3.4.2	Network Management Reliability is a conditional requirement for a VALAN .[1]
			Security	Met	GSCR, Appendix 3, A.3.3.4.3	See note 2.
			IPv6	Met	GSCR, Paragraph 1.7, and Appendix 3, A3.2.8	See note 3.
			TE	Met	GSCR, Appendix 3, A.3.3.4.4	For a VALAN, redundant links are not required.[1]

Table 2-6. Component Interoperability Test Summary (continued)

DSN Line Interfaces						
Interface	**Component**	**Status**	**Device Requirement**	**Test Results**	**Reference**	**Remarks**
1000/10000 BaseFX 10/100/1000 BaseTX	**Foundry BigIron RX** 4/**8**/16/32	Certified as: Distribution Access	CoS Models	Met	GSCR, Appendix 3, A3.3.2.1	
			Traffic Prioritization	Met	GSCR, Appendix 3, A3.3.2.2	
			QoS	Met	GSCR, Appendix 3, A3.3.3	
			Policing	Met	GSCR, Appendix 3, A3.3.3.2	
			VLANs	Met	GSCR, Appendix 3, A3.3.3.3	
			IEEE Conformance	Met	GSCR, Appendix 3, A3.3.4	
			Reliability	Met	GSCR, Appendix 3, A3.3.4.1	Reliability is a conditional requirement for a VALAN .[1]
			Network Management	Met	GSCR, Appendix 3, A.3.3.4.2	Network Management Reliability is a conditional requirement for a VALAN .[1]
			Security	Met	GSCR, Appendix 3, A.3.3.4.3	See note 2.
			IPv6	Met	GSCR, Paragraph 1.7, and Appendix 3, A3.2.8	See note 3.
			TE	Met	GSCR, Appendix 3, A.3.3.4.4	For a VALAN, redundant links are not required.[1]
1000BaseFX 10/100 BaseTX	**Foundry BigIron 4000**/8000/15000 Switches	Certified as: Distribution Access	CoS Models	Met	GSCR, Appendix 3, A3.3.2.1	
			Traffic Prioritization	Met	GSCR, Appendix 3, A3.3.2.2	
			QoS	Met	GSCR, Appendix 3, A3.3.3	
			Policing	Met	GSCR, Appendix 3, A3.3.3.2	
			VLANs	Met	GSCR, Appendix 3, A3.3.3.3	
			IEEE Conformance	Met	GSCR, Appendix 3, A3.3.4	
			Reliability	Met	GSCR, Appendix 3, A3.3.4.1	Reliability is a conditional requirement for a VALAN .[1]
			Network Management	Met	GSCR, Appendix 3, A.3.3.4.2	Network Management Reliability is a conditional requirement for a VALAN .[1]
			Security	Met	GSCR, Appendix 3, A.3.3.4.3	See note 2.
			IPv6	Met	GSCR, Paragraph 1.7, and Appendix 3, A3.2.8	See notes 3 and 4.
			TE	Met	GSCR, Appendix 3, A.3.3.4.4	For a VALAN, redundant links are not required.[1]

Table 2-6. Component Interoperability Test Summary (continued)

DSN Line Interfaces						
Interface	**Component**	**Status**	**Device Requirement**	**Test Results**	**Reference**	**Remarks**
1000/10000 BaseFX 10/100/1000 BaseTX	**FastIron SX 800**/SX 1600 Switches	Certified as: Access	CoS Models	Met	GSCR, Appendix 3, A3.3.2.1	
			Traffic Prioritization	Met	GSCR, Appendix 3, A3.3.2.2	
			QoS	Met	GSCR, Appendix 3, A3.3.3	
			Policing	Met	GSCR, Appendix 3, A3.3.3.2	
			VLANs	Met	GSCR, Appendix 3, A3.3.3.3	
			IEEE Conformance	Met	GSCR, Appendix 3, A3.3.4	
			Reliability	Met	GSCR, Appendix 3, A3.3.4.1	Reliability is a conditional requirement for a VALAN .[1]
			Network Management	Met	GSCR, Appendix 3, A.3.3.4.2	Network Management Reliability is a conditional requirement for a VALAN .[1]
			Security	Met	GSCR, Appendix 3, A.3.3.4.3	See note 2.
			IPv6	Met	GSCR, Paragraph 1.7, and Appendix 3, A3.2.8	See note 3.
			TE	Met	GSCR, Appendix 3, A.3.3.4.4	For a VALAN, redundant links are not required.[1]
1000BaseFX 10/100/1000 BaseTX	**FastIron Edge X** FESX424 **FESX424-PoE** FESX424HF FESX448	Certified as: Access	CoS Models	Met	GSCR, Appendix 3, A3.3.2.1	
			Traffic Prioritization	Met	GSCR, Appendix 3, A3.3.2.2	
			QoS	Met	GSCR, Appendix 3, A3.3.3	
			Policing	Met	GSCR, Appendix 3, A3.3.3.2	
			VLANs	Met	GSCR, Appendix 3, A3.3.3.3	
			IEEE Conformance	Met	GSCR, Appendix 3, A3.3.4	
			Reliability	Met	GSCR, Appendix 3, A3.3.4.1	Reliability is a conditional requirement for a VALAN .[1]
			Network Management	Met	GSCR, Appendix 3, A.3.3.4.2	Network Management Reliability is a conditional requirement for a VALAN .[1]
			Security	Met	GSCR, Appendix 3, A.3.3.4.3	See note 2.
			IPv6	Met	GSCR, Paragraph 1.7, and Appendix 3, A3.2.8	See note 3.
			TE	Met	GSCR, Appendix 3, A.3.3.4.4	For a VALAN, redundant links are not required.[1]

Table 2-6. Component Interoperability Test Summary (continued)

DSN Line Interfaces						
Interface	**Component**	**Status**	**Device Requirement**	**Test Results**	**Reference**	**Remarks**
1000BaseFX 10/100/1000 BaseTX	**FastIron GS** / LS **GS648P-PoE** GS624P-PoE LS648 LS624	Certified as: Access	CoS Models	Met	GSCR, Appendix 3, A3.3.2.1	
			Traffic Prioritization	Met	GSCR, Appendix 3, A3.3.2.2	
			QoS	Met	GSCR, Appendix 3, A3.3.3	
			Policing	Met	GSCR, Appendix 3, A3.3.3.2	
			VLANs	Met	GSCR, Appendix 3, A3.3.3.3	
			IEEE Conformance	Met	GSCR, Appendix 3, A3.3.4	
			Reliability	Met	GSCR, Appendix 3, A3.3.4.1	Reliability is a conditional requirement for a VALAN .[1]
			Network Management	Met	GSCR, Appendix 3, A.3.3.4.2	Network Management Reliability is a conditional requirement for a VALAN .[1]
			Security	Met	GSCR, Appendix 3, A.3.3.4.3	See note 2.
			IPv6	Met	GSCR, Paragraph 1.7, and Appendix 3, A3.2.8	See note 3.
			TE	Met	GSCR, Appendix 3, A.3.3.4.4	For a VALAN, redundant links are not required.[1]
1000BaseFX 10/100 BaseTX	**FastIron Edge 4802-PoE** 2402-PoE	Certified as: Access	CoS Models	Met	GSCR, Appendix 3, A3.3.2.1	
			Traffic Prioritization	Met	GSCR, Appendix 3, A3.3.2.2	
			QoS	Met	GSCR, Appendix 3, A3.3.3	
			Policing	Met	GSCR, Appendix 3, A3.3.3.2	
			VLANs	Met	GSCR, Appendix 3, A3.3.3.3	
			IEEE Conformance	Met	GSCR, Appendix 3, A3.3.4	
			Reliability	Met	GSCR, Appendix 3, A3.3.4.1	Reliability is a conditional requirement for a VALAN .[1]
			Network Management	Met	GSCR, Appendix 3, A.3.3.4.2	Network Management Reliability is a conditional requirement for a VALAN .[1]
			Security	Met	GSCR, Appendix 3, A.3.3.4.3	See note 2.
			IPv6	Met	GSCR, Paragraph 1.7, and Appendix 3, A3.2.8	See notes 3 and 5.
			TE	Met	GSCR, Appendix 3, A.3.3.4.4	For a VALAN, redundant links are not required.[1]

Table 2-6. Component Interoperability Test Summary (continued)

LEGEND:

10/100BaseTX	- 100/1000 Mbps Ethernet over Category 5 Twisted Pair Copper
1000BaseFX	- 1000 Mbps Ethernet over fiber
ACL	- Access Control List
ASVALAN	- Assured Services Voice Application Local Area Network
CoS	- Class of Service
DISA	- Defense Information Systems Agency
DISR	- DoD Information Technology Standards Registry
DoD	- Department of Defense
GSCR	- Generic Switching Center Requirements
IEEE	- Institute of Electrical and Electronics Engineers, Inc.
IPv4	- Internet Protocol version 4
IPv6	- Internet Protocol version 6
Mbps	- Megabits per second
QoS	- Quality of Service
TE	- Traffic Engineering
VALAN	- Voice Application Local Area Network
VLAN	- Virtual Local Area Network

NOTES:

1 If a system meets the requirements for an ASVALAN, it also meets the lesser requirements for a VALAN.

2 Security is tested by DISA-led Information Assurance test teams and published in a separate report.

3 An IPv6 capable system or product, as defined in the GSCR, paragraph 1.7, shall be capable of receiving, processing, and forwarding IPv6 packets and/or interfacing with other systems and protocols in a manner similar to that of IPv4. IPv6 capability is currently satisfied by a vendor Letter of Compliance signed by the Vice President of the company. The vendor must state, in writing, compliance to the following criteria:
   a. Conformant with IPv6 standards profile contained in the DISR.
   b. Maintaining interoperability in heterogeneous environments and with IPv4.
   c. Commitment to upgrade as the IPv6 standard evolves.
   d. Availability of contractor/vendor IPv6 technical support.

4 The BigIron series met all IPv4 requirements. Support for IPv6 is limited to 50,000 packets per second throughput, total of all aggregates, with the ACL enabled. With the ACL disabled, it met all IPv6 requirements without limitation. The ACL must remain enabled if the BigIron series is used as an access layer device. Currently, there is no defined minimum requirement for packets per second.

5 The FastIron Edge series met all IPv4 requirements. Support for IPv6 is limited to 50,000 packets per second throughput, total of all aggregates, with the ACL enabled. Since the FastIron Edge series is certified just for the access layer, the ACL must remain enabled. Currently, there is no defined minimum requirement for packets per second.

12. TEST AND ANALYSIS REPORT. No detailed test report was developed in accordance with the Program Manager's request. JITC distributes interoperability information via the JITC Electronic Report Distribution (ERD) system, which uses Unclassified-But-Sensitive Internet Protocol Router Network (NIPRNet) e-mail. More comprehensive interoperability status information is available via the JITC System Tracking Program (STP). The STP is accessible by .mil/gov users on the NIPRNet at https://stp.fhu.disa.mil. Test reports, lessons learned, and related testing documents and references are on the JITC Joint Interoperability Tool (JIT) at https://jit.fhu.disa.mil (NIPRNet), or http://199.208.204.125 (SIPRNet). Information related to DSN testing is on the Telecom Switched Services Interoperability (TSSI) website at http://jitc.fhu.disa.mil/tssi.